КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

UDC 004.056.2
DOI https://doi.org/10.32782/2521-6643-2024-1-67.11

Voskoboinyk V. O., Candidate of Technical Sciences,
Associate Professor, Professor at the Department
of Information Security and Nanoelectronics
Zaporizhzhia Polytechnic National University
ORCID: 0000-0003-3786-8666

Savchenko Iu. V., Candidate of Technical Sciences,
Associate Professor,
Associate Professor at the Department of cybersecurity
and Information technology
University of Customs and Finance
ORCID: 0000-0002-7177-6311

Karpukov L. M., Doctor of Technical Sciences, Professor,
Professor at the Department of Information Security
and Nanoelectronics
Zaporizhzhia Polytechnic National University
ORCID: 0000-0002-7098-6018

Parshyna O. A., Doctor of Economic Sciences, Professor,
Professor at the Department of cybersecurity
and Information technology
University of Customs and Finance
ORCID: 0000-0002-7836-0140

Prokopovych-Tkachenko D. I., Candidate of Technical Sciences,
Associate Professor, Associate Professor at the Department
of Cyber Security and Information Technologies,
University of Customs and Finance
ORCID: 0000-0002-6590-3898

ASSESSMENT OF THE STATE OF INFORMATION SECURITY USING EXPERT SYSTEMS

The problems considered in the article are related to ensuring the specified indicators of efficiency and reliability of the designed software complexes for information systems through a structural approach to the main stages of the software life cycle. The relevance of this class of software is determined by the wide distribution of such systems. Distinctive features of the modern complex of programs for information systems are their large information and logical complexity, significant volumes of programs, work in conditions of a limited amount of computing resources with high requirements for the efficiency and reliability of their functioning, as well as a pronounced production and technical nature of software tools for all life cycle stages. The main problem associated with the creation of complex software systems is to increase the reliability of programs. One of the promising ways to solve the problem is the implementation of a detailed regulated technological process. At the same time, the required level of regulation has been achieved as a result of a structural approach to ensuring reliability at various stages of software life. Among the known ways to improve the reliability of software, this article pays special attention to progressive methods of creating programs and the widespread use of automation tools, since the technology under consideration and its instrumental support are based on a structural approach to software development. The role and influence of the corresponding structural methods on the reliability characteristics of the software is shown. In general, the structural approach makes it possible to increase the efficiency of working with software based on the implementation of three provisions: streamlining and unifying the structural construction of the software package; ordering work to eliminate errors; creating conditions for the effective application of assembly programming technology based on the software backlog.

Key words: *information systems, reliability, efficiency, software, quality, structure, technological process, integrated indicator, objective function, errors, probability of failures, cybersecurity.*

Воскобойник В. О., Савченко Ю. В., Карпуков Л. М., Паршина О. А., Прокопович-Ткаченко Д. І. Оцінка стану інформаційної безпеки за допомогою експертних систем

Розглянуті в статті проблеми пов'язані із забезпеченням кібербезпеки інформації та заданих показників ефективності та надійності проєктованих програмних комплексів для інформаційних систем за рахунок структурного підходу до основних етапів життєвого циклу програмного забезпечення. Актуальність даного класу програмного забезпечення визначається широким розповсюдженням таких систем. Відмінними рисами сучасного комплексу програм для інформаційних систем є їх велика інформаційна та логічна складність, значні обсяги програм, робота в умовах обмеженої кількості обчислювальних ресурсів при високих вимогах до ефективності та надійності їх функціонування, а також яскраво виражений виробничо-технічний характер програмних засобів на всіх етапах життєвого циклу. Основною проблемою, пов'язаною зі створенням складних програмних систем, є підвищення надійності програм. Одним з перспективних шляхів вирішення проблеми є реалізація детально регламентованого технологічного процесу. При цьому необхідний рівень регламентації досягається в результаті структурного підходу до забезпечення надійності на різних етапах життя програмного забезпечення. Серед відомих шляхів підвищення надійності ПЗ в даній статті особлива увага приділяється прогресивним методам створення програм та широкому використанню засобів автоматизації, оскільки розглянута технологія та її інструментальна підтримка ґрунтується на структурному підході до розробки ПЗ. Показано роль та вплив відповідних структурних методів на характеристики надійності ПЗ. В цілому структурний підхід дозволяє підвищити ефективність роботи з програмним забезпеченням на основі реалізації трьох положень: впорядкування та уніфікації структурної побудови програмного комплексу; впорядкування робіт з усунення помилок; створення умов для ефективного застосування технології програмування на основі відставання програмного забезпечення використовуючи мову Асемблер.

Ключові слова: *інформаційні системи, надійність, ефективність, програмне забезпечення, якість, структура, технологічний процес, інтегральний показник, цільова функція, помилки, ймовірність відмов, кібербезпека.*

Introduction. The development of the modern world is characterized by various regular trends. One of them, and a very important one, is the increasing importance of the available information types. In this regard, in the period of society informatization, one of the urgent problems is information security. Various subjects of economic, state and information relations, such as the state, many public organizations, solid commercial organizations, as well as enterprises and citizens, as the main constituent unit of the state, need to form information security and ensure their information systems with it. The main objectives for ensuring information security are: minimizing the financial costs generated in the process of implementing threats, full compliance with the requirements of state regulatory bodies, ensuring the unity and integrity, as well as confidentiality and availability of information. It should be emphasized that those organizations that do not pay due attention to information security issues face constant failures and problems in their work and suffer huge material and financial losses. It is much easier and cheaper to ensure reliable information security than to eliminate the severe consequences of threats [1].

Successful information security requires a comprehensive approach to information security [2].

The problem of software reliability is of particular importance for real-time information systems operated for a long period of time under extreme loads. First of all, they highlight the tasks associated with the choice and practical definition of quality indicators and quality assessment criteria, the tasks of analyzing the complexity of programs and creating methods for targeted management of the complexity and quality of programs, as well as creating methods for managing the development of programs. The experience of creating information systems and their operation led to the formation of such a direction as software reliability.

Despite the commonality of the main provisions of software reliability and hardware reliability, there is a fundamental difference in the causes of software malfunctions [1-3, 15]. With regard to software, this reason is that the real data to be processed cannot be processed by a specific program focused on this type of processing. This is due to the fact that the initial data, being in the range of acceptable values, nevertheless, did not fall into the area verified during testing and testing. Under the primary error, as a rule, is understood [4], [5] the deviation of the source text of the program from the formalized reference and customer requirements. Distortions in the program are those of its elements that are subject to correction. The primary error appears when comparing the results of program execution with some standard.

The main tasks of the reliability of information systems software are [6] – [8] as follows:

– formation of the basic concepts used in the study of indicators and parameters of software reliability;

– identification and study of the main factors that determine the characteristics of the reliability of programs;

– study of the characteristics of distortions of the initial data from various types of sources and their impact on the reliability of the programs;

– study of types of errors in programs and the dynamics of changes in their number during debugging;

– development and research of design methods and structural construction of complex programs that improve the reliability of operation;

– study of means and methods of control and protection against distortions of the computing process by introducing various types of redundancy and noise immunity, providing automatic recovery to the original state;

– development of methods for predicting reliability characteristics.

The main part of the article. The article deals with the issues aimed at solving the most urgent problem of modern society in the conditions of widespread informatization – information security, especially in the conditions of information warfare [3].

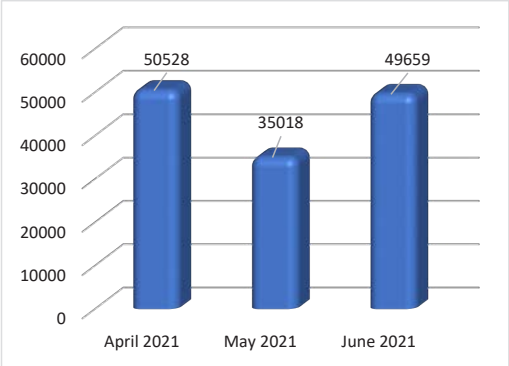

Fig. 1. Statistics of financial threats

The statistics presented here are based on the defect products provided by users who have confirmed their consent to the transfer of statistical data. Thus, in the second quarter of 2021 119,252 computers were prevented from launching one or more malware designed to steal money from bank accounts (Fig. 1) [4].

Traditionally, ZeuS/Zbot has become one of the most widespread bunker families (17.8%), but its share has almost halved, down 13 pp. CliptoShuffler (9.9%) took second place again, with its share also decreasing by 6 percentage points. The top three is rounded off by SpyEye (8.8%), which gained 5 percentage points and, as a result, moved up from 8th place. It is also worth noting the disappearance of Emotet from the TOP 10, which is a predictable event given the liquidation of the banker's infrastructure in the previous quarter [5]. Targeted ransomware attacks on large organizations continued in the second quarter. Perhaps the most high-profile event of the quarter was the attack by DarkSide ransomware on Colonial Pipeline, one of the largest fuel pipeline operators in the United States. The incident resulted in fuel disruptions and the declaration of a state of emergency in four states. The attack was investigated by the FBI and several other US government organizations, and the incident was reported to US President Biden [6].

For the attackers, such sudden fame was unwelcome. The creators of DarkSide published a post on their blog blaming "third-party" operators. Later, another post was published stating that DarkSide developers had lost access to part of their infrastructure and were closing the service and affiliate programmed. Another consequence of this high-profile incident was a new rule on the XSS forum, where many encryption developers, including REvil (also known as Sodinokibi or Sodin), LockBit, and Netwalker, advertise their affiliate programmed [7]. According to the new rule, the forum's administration has banned the advertising and sale of any ransomware on the site. A similar decision was made on other forums popular with criminals. Ukrainian police conducted searches and arrested members of the Clop group. The law enforcement agencies also deactivated part of the group's infrastructure, which, however, did not lead to the suspension of the group's activities. In the second quarter, attackers targeting network attached storage (NAS) devices became more active. A new family of Qlocker ransomware was introduced that packs user files into a password-protected 7zip archive, while old friends ech0raix and AgeLocker gained momentum and protected 97,451 users from ransomware attacks [8].

In the first quarter of 2023, a list of the most active extortion groups, i.e., those who have added the most victims to their site are presented in Fig. 2. [9]

The process of digitalization of modern society raises problems associated with the possibility of unauthorized access to critical facility resources. The security of critical facility resources is of great importance for ensuring the effective functioning of both an individual enterprise and the entire state. Therefore, the issue of developing and implementing a system for assessing the level of information security is certainly relevant.

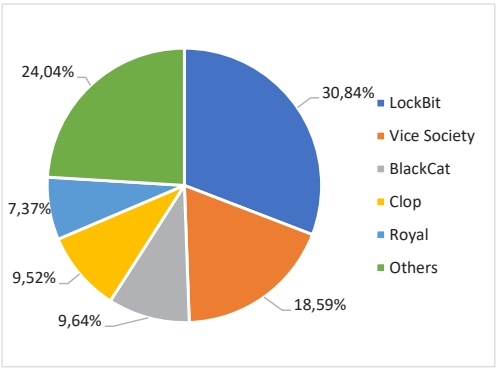

Fig. 2. List of the most active extortion groups

An important condition for the effective operation of a critical facility resource protection system is its manageability. A modern CIP resource protection system has a complex, multi-component, physically and logically distributed structure. The design of an optimal protection system involves the use of qualitative and quantitative information about the importance of criteria and the construction of a multi-criteria generalized decision-making criterion for critical infrastructure facilities, which is based on a certain set of necessary subsystems-modules, such as: a module for protecting the network perimeter and inter-network interactions, a module for protecting network servers, workstation protection, a module for comprehensive anti-virus protection, cryptographic protection, etc.

Closely related to the concept of program reliability is the concept of errors in programs. The results of the analysis of errors in programs [9], [10] showed that complex software cannot exist in an absolutely debugged state. Errors [11-13] introduced into programs during design, development, and implementation are sources of software reliability degradation. At the stage of structural design, errors in determining the structure of programs are possible.

The relationship between the number of expected and remaining errors at the end of the technological cycle with system reliability indicators is often determined by the specifics of the area of program use. In the general case, the system reliability indicator of programs is the probability of failure-free operation during the time interval t, i.e., until the first failure occurs:

$$P(t) = P(T \geq t) \tag{1}$$

The probability of failure-free operation allows you to determine the following system indicators:

$$\Theta(t) = 1 - P(t); \tag{2}$$

$$a(t) = \Theta\,(t) = 1 - P'(t); \tag{3}$$

$$\lambda(t) = a(t)/[P(t)] = d\ lnP(t)/d(t). \tag{4}$$

Most of the indicators specified by individual software components and technological operations are associated with these system indicators.

The use of various mathematical reliability models designed to assess program reliability indicators (for example, the number of errors remaining undetected; the time required to detect the next error; the time required to detect all errors with a given probability, etc.) allows for a more reasonable approach to planning debugging and testing programs, deeper understanding of the nature of errors and methods for their prevention, methods for the effective use of redundancy. Each of these models is based on some assumptions and is focused on a certain class of programs.

Among these types of errors that reduce the reliability of programs, a special place is occupied by primary errors, which are distortions in the source code of the program. Since the primary errors in programs are introduced into their source texts, a special place for evaluating software reliability is given to a method based on the analysis and control of the statistical characteristics of program source texts.

The use of the structural approach as the basis for the regulation of the technological process and the constructive organization of programs has a twofold character. On the one hand, structuring leads to an increase in the reliability of programs. On the other hand, structuring leads to an increase in costs and is associated with certain losses in the characteristics of programs, which negatively affects their reliability. For a comparative assessment and comparison of the two directions of action of structuring, a simplified model of the relationship between program structuring and their reliability is proposed, which makes it possible to draw a qualitative conclusion about the nature of this dependence [14, 16, 17].

Assuming that the total increment in the number of program elements during structuring is evenly distributed among each M modules, we denote the average increment per module as A:

$$A = \Delta N / M,$$

where ΔN – increase in the number of program elements due to structuring.

To simplify the distribution of errors over all elements of the program, let us assume that the error rate K per element of the program is constant, i.e.

$$K = n / N = \text{const},$$

where n – number of errors in a monolithic software package.

Let's introduce the notion of error search length L, considering that in order to find errors it is necessary to look through all N elements of the program complex. Then the length of the search for n errors is

$$L = N\,n = N^2K.$$

The length of the structured set of programs is considered evenly distributed on M modules, the length of each module is equal to $(N + AM) / M$. The number of errors in the structured set of programs will be $(N + AM)\,K$, then the number of errors per module will be on average equal to $(N+AM)\,K / M$.

The search for errors attributable to each module occurs only within the module. This assumption is based on the fact that structuring aims at maximum automation of each module. Thus, the search length L_c of all errors in a structured set of programs is determined by the relation

$$L_c = \frac{N + AM}{M} = \frac{(N + AM)KM}{M} = \frac{(N + AM)^2 K}{M}$$

characterizing the relationship between the search length of the total number of errors.

As the total number of elements in the structuring and, consequently, the number of errors in the program complex M and A increase, the values at which the error search length in the structured complex is less than the error search length in the monolithic program complex acquire such values. To determine the conditions under which $L_c < L$, we can introduce a characteristic of the length of a program module $N_o = N / M$.

Solving the system of equations:

$$L_c = M (N_o + A)^2 K;$$

$$L = K N_o^2 M^2,$$

we obtain that $L_c < L$, when $M > (1 + AN / N)^2$. It follows that even if the volume of a structured program complex is doubled, its length will be less.

The technological process of software creation can be represented as a set of operations obtained as a result of detailing of the regulated sequence of stages and phases as applied to specific conditions of technology use. Such regulation and detailing of the technological process of software creation is aimed, first of all, at achieving the specified technical quality indicators. In the overall technological scheme, you can present the purpose of each stage and operation in the implementation of various components of quality indicators, and then form an integrated indicator. Such an integrated indicator of the quality of the created software can be defined in the form of the ratio $\Pi = F(\Pi_l)$ where $l = 1 \ldots m$ – parameter number; Π_l – value of the l-th quality parameter; m – the number of used indicators. Given the contribution and role of each technological step or operation in achieving a given indicator, we can derive a relationship to determine each l-th quality indicator in the form of $\Pi_l = F(\Pi_{li})$, where $i = 1 \ldots \kappa$ – current issue; κ – number of steps and operations. The goal of the technological process is to optimize by some predetermined criterion the value of the integral quality indicator:

$$Pr = \text{opt}[\Phi(F(\Pi_{li}))]; \; l = 1 \ldots m; \; i = 1 \ldots \kappa.$$

The specific type of functions F and Φ is determined by the type of the corresponding indicators and the features of the technology. The degree of achieving the target function of the technology determines its quality.

The formalized relations introduced allow us to conduct quantitative evaluations when choosing specific technologies for software creation. At the same time the system indicator of reliability is the probability of faulty program operation P_l – is defined by the relation

$$P_l = F(\Pi_{ij}) = \prod_{i=1}^{k} P_i$$

i.e., the product of the probabilities of no-failure operation, calculated according to the formula (1), achieved at each technological stage. With regard to the quality indicators under consideration, the target function takes the form of

$$Pr = max \prod_{i=1}^{k} P_i$$

where P_i is calculated using the formula (1).

Where P_i is calculated by formula (1). Similarly for each technological stage we can calculate the remaining reliability indexes $\Theta(t)$, $a(t)$, $\lambda(t)$ according to formulas (2) – (4) respectively.

When using the reliability indicators detailed by technological operations, the target function takes into account the integration of the system indicator. It is shown that all errors can be assigned to four classes of available programs in complexes. The figure shows these classes and their percentage ratio, as well as the main groups of errors prevented by the structuring methodology.

All technologies and automation tools that support the process of creating software for information systems should focus on solving the problem of increasing the reliability of operation. Currently, significant results have been achieved in the study of these problems, which allow us to identify ways of improving the reliability of this class of programs:

– development of a methodological theory of software reliability, including research of methods of software reliability analysis, selection and justification of criteria, study of error types, causes of their occurrence and distribution laws;

– development and implementation of software methods for designing complex programs;

– development of methods for evaluation and prediction of reliability characteristics, especially at early stages of software creation, methods for timely error prevention and localization, methods for measuring statistical characteristics that determine the stability of functioning and software reliability;

– development of methods for maintaining programs and their modernization under conditions of long-term operation.

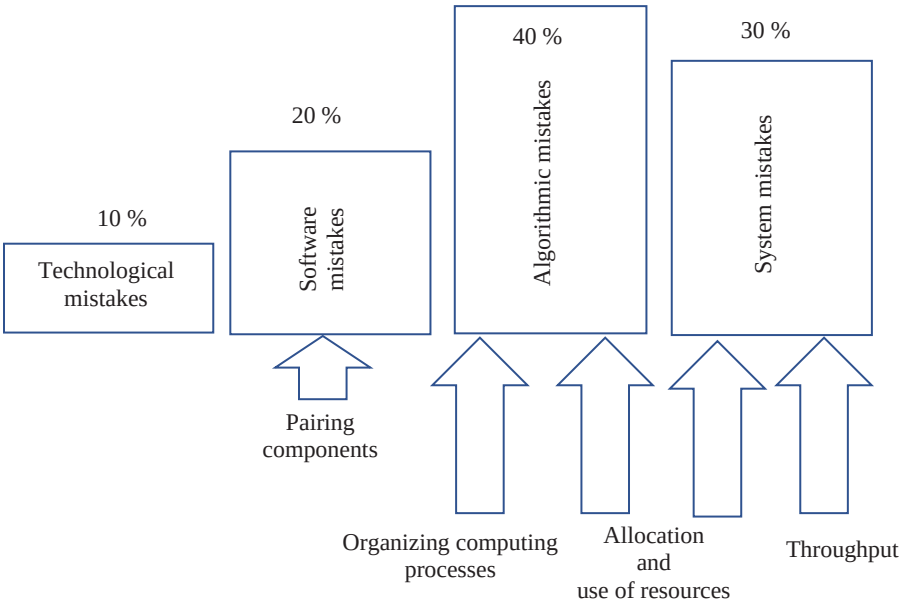

Fig. 3. Groups of errors prevented by structural design

The main result of the authors' research is structuring the types of software errors fig. 3. As a result of the structural approach to the design, the integrated software quality index is defined and the technological process goal is formulated, which is to optimize by some predetermined criterion the value of the integral quality index.

Complex practical decision-making tasks of critical facilities are usually multi-criteria: the consequences of decisions have to be assessed using not one, but several criteria (indicators of quality or efficiency of target functions).

To analyze complex and responsible multi-criteria decision-making tasks, the experience, knowledge and intuition of the decision maker and experts are not enough. It is necessary not only to have adequate information support, but also to use special mathematical methods developed by decision-making theory.

To select the best (optimal) solution, it is not enough to set a set of criteria. Additional information about the preferences of the decision maker is needed, which should be formally represented in the model of the problem situation.

Conclusions. The article considers the issues aimed at resolving the most pressing problem of modern society in the conditions of widespread informatization – information security, especially in the conditions of information warfare.

Modern expert systems are developed using the mathematical apparatus of fuzzy logic for operation in narrow areas of application and are designed to solve quite complex problems based on the experience of experts' work constantly accumulated in the knowledge base, to recreate the experience, knowledge of high-level professionals and use this knowledge. Practical implementation of expert systems allows, on the basis of the facts provided by the user, to recognize a situation, formulate a decision or give a recommendation for the choice of action and consists in making the optimal decision for effective information security. Nowadays, expert systems can be widely enough used in analyzing and assessing the state of information security by specialists of any qualification. Using expert systems with new knowledge bases on normative documents in the field of information protection, with specific solutions for many realistically possible situations, it is possible to greatly simplify the work of information security specialists in many organizations and at the same time provide them with self-training on specific examples, as on a kind of simulator

It should be emphasized that due to high financial, labour, social and time costs, expert systems are currently not widespread. Although in the field of information technologies everything is changing very quickly, in the near future the labour and experience of human professionals will not be replaced by the work of artificial intelligence, including ES. Today, expert systems can achieve significant results by functioning and interacting only together with humans, because it is man, unlike artificial intelligence, who is able to analyses, think, think creatively and non-standard, and this allows him to develop and move forward throughout his era.

To select the best (optimal) solution, it is not enough to set a set of criteria.

The results of the study are necessary for the development of complex software complexes of information systems. The methodology of structural design of complex software already at the design stage, presented in the article, allows to prevent a significant number of errors due to the detailing of reliability indicators by technological operations.

Complex practical decision-making tasks of critical facilities are usually multi-criteria: the consequences of decisions have to be assessed using not one, but several criteria (indicators of quality or efficiency of target functions).

To analyze complex and responsible multi-criteria decision-making tasks, the experience, knowledge and intuition of the decision maker and experts are not enough. It is necessary not only to have adequate information support, but also to use special mathematical methods developed by decision-making theory.

To select the best (optimal) solution, it is not enough to set a set of criteria. Additional information about the preferences of the decision maker is needed, which should be formally represented in the model of the problem situation.

Bibliography:

1. I. Savchenko, O. Shapoval, T. Chupilko, Y. Ulianovska, V. Titov, and V. Shchepetov. "Computer Simulation of Safety Processes of Composite Structures Rheological Properties.". (2022) doi:10.1109/MEES58014.2022.10005747

2. I. Savchenko, O. Shapoval, V. Bakharev, T. Chupilko, M. Babaryka, and N. Dzyna. "Mathematical Model of Rheological Processes of Composite Materials Deformation.". (2022) doi:10.1109/MEES58014.2022.10005658

3. O. Khrebtova, O. Shapoval, O. Markov, V. Kukhar, N. Hrudkina, and M. Rudych. "Control Systems for the Temperature Field during Drawing, Taking into Account the Dynamic Modes of the Technological Installation.". (2022) doi:10.1109/MEES58014.2022.10005724

4. V. Kulynych, A. Shapoval, and V. Dragobetskii. Hard Alloys Recycling as a Promising Direction of Technological Equipment for Machine-Building Production. Materials Science Forum. Vol. 1052 MSF (2022). doi:10.4028/p-49mxgo

5. Parshina O., Savchenko Yu., Polyanovs`ka B. Problem aspects of financial and economic security in the conditions of development crypt. Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. Special Issue № 1. 2019. pp. 243–248. DOI: 10.31733/2078-3566-2019-5-243-249.

6. Паршина О.А., Паршин Ю.І., Савченко Ю.В. Економічна безпека в умовах діджиталізації: сучасний стан та перспективи розвитку інформаційного суспільства. Науковий вісник Дніпропетровського державного університету внутрішніх справ: Зб. наук. праць. 2019. № 2. С. 148–155.

7. Паршина О.А., Паршин Ю.І., Савченко Ю.В. Система менеджменту забезпечення конкурентоспроможності промислової продукції в умовах дефіцитності ресурсів. Східна Європа: економіка, бізнес та управління. 2019. №6 (23). С. 354–359. URL: (http://www.easterneurope-ebm.in.ua/journal/23_2019/55.pdf)

8. V. Dragobetskii, V. Zagirnyak, S. Shlyk, A. Shapoval, and O. Naumova. "Application of Explosion Treatment Methods for Production Items of Powder Materials." Przeglad Elektrotechniczny 95 (5): 39-42 (2019.). doi:10.15199/48.2019.05.10

9. M. Zagirnyak, V. Zagirnyak, D. Moloshtan, V. Drahobetskyi, and A. Shapoval. "A Search for Technologies Implementing a High Fighting Efficiency of the Multilayered Elements of Military Equipment." Eastern-European Journal of Enterprise Technologies 6 (1-102): 33-40 (2019). doi:10.15587/1729-4061.2019.183269

10. S.G. Karnaukh, O.E. Markov, V.V. Kukhar, and A.A. Shapoval. 2022. "Classification of Steels According to their Sensitivity to Fracture using a Synergetic Model." Int J Adv M Tech 119 (7-8): 5277-5287. (2022) doi:10.1007/s00170-022-08653-y

11. I. Lutsenko "Identification of Target System Operations. Development of Global Efficiency Criterion of Target Operations." Eastern-European Journal of Enterprise Technologies 2 (2): 35-40. (2015.) doi:10.15587/1729-4061.2015.38963

12. M.V. Zagirnyak, V.V. Prus, and A.V. Nikitina. "Grounds for Efficiency and Prospect of the use of Instantaneous Power Components in Electric Systems Diagnostics." Przeglad Elektrotechniczny 82 (12): 123-125 (2006.)

13. Savchenko, I., Shapoval, A., Kuziev, I. Modeling of high module power sources systems safety processes. (2022) Materials Science Forum, 1052 MSF, pp. 399-404.

14. Savchenko, I., Shapoval, O., Kozechko, V., Markov, O., Hrudkina, N., Voskoboynik, V. Optimization of Informative Signals Stability Along the Waveguides. (2021) Proceedings of the 20th IEEE International Conference on Modern Electrical and Energy Systems, MEES 2021.

15. Hrudkina, N. S., O. E. Markov, A. A. Shapoval, V. A. Titov, I. S. Aliiev, P. Abhari, and K. V. Malii. (2022). "Mathematical and Computer Simulation for the Appearance of Dimple Defect by Cold Combined Extrusion." FME Transactions 50 (1): 90-98. doi:10.5937/fme2201090H

16. O.E. Markov "Forging of Large Pieces by Tapered Faces." Steel in Translation 42 (12): 808-810. (2012.) doi:10.3103/S0967091212120054

References:

1. I. Savchenko, O. Shapoval, T. Chupilko, Y. Ulianovska, V. Titov, and V. Shchepetov. "Computer Simulation of Safety Processes of Composite Structures Rheological Properties.". (2022) doi:10.1109/MEES58014.2022.10005747

2. I. Savchenko, O. Shapoval, V. Bakharev, T. Chupilko, M. Babaryka, and N. Dzyna. "Mathematical Model of Rheological Processes of Composite Materials Deformation.". (2022) doi:10.1109/MEES58014.2022.10005658

3. O. Khrebtova, O. Shapoval, O. Markov, V. Kukhar, N. Hrudkina, and M. Rudych. "Control Systems for the Temperature Field during Drawing, Taking into Account the Dynamic Modes of the Technological Installation.". (2022) doi:10.1109/MEES58014.2022.10005724

4. V. Kulynych, A. Shapoval, and V. Dragobetskii. Hard Alloys Recycling as a Promising Direction of Technological Equipment for Machine-Building Production. Materials Science Forum. Vol. 1052 MSF (2022). doi:10.4028/p-49mxgo

5. Parshina O., Savchenko Yu., Polyanovs`ka B. Problem aspects of financial and economic security in the conditions of development crypt. Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. Special Issue № 1. 2019. pp. 243–248. DOI: 10.31733/2078-3566-2019-5-243-249.

6. Parshina O.A., Parshin Y.I., Savchenko Y.V. Economic security in the context of digitalization: current state and prospects for the development of the information society. Scientific Bulletin of Dnipropetrovs'k State University of Internal Affairs: Collection of scientific works. 2019. № 2. С. 148-155.

7. Parshina O.A., Parshin Y.I., Savchenko Y.V. Management system for ensuring the competitiveness of industrial products in conditions of resource scarcity. Eastern Europe: economy, business and management. 2019. №6 (23). С. 354-359. URL: (http://www.easterneurope-ebm.in.ua/journal/23_2019/55.pdf)

8. V. Dragobetskii, V. Zagirnyak, S. Shlyk, A. Shapoval, and O. Naumova. "Application of Explosion Treatment Methods for Production Items of Powder Materials." Przeglad Elektrotechniczny 95 (5): 39-42 (2019.). doi:10.15199/48.2019.05.10

9. M. Zagirnyak, V. Zagirnyak, D. Moloshtan, V. Drahobetskyi, and A. Shapoval. "A Search for Technologies Implementing a High Fighting Efficiency of the Multilayered Elements of Military Equipment." Eastern-European Journal of Enterprise Technologies 6 (1-102): 33-40 (2019). doi:10.15587/1729-4061.2019.183269

10. S.G. Karnaukh, O.E. Markov, V.V. Kukhar, and A.A. Shapoval. 2022. "Classification of Steels According to their Sensitivity to Fracture using a Synergetic Model." Int J Adv M Tech 119 (7-8): 5277-5287. (2022) doi:10.1007/s00170-022-08653-y

11. I. Lutsenko "Identification of Target System Operations. Development of Global Efficiency Criterion of Target Operations." Eastern-European Journal of Enterprise Technologies 2 (2): 35-40. (2015.) doi:10.15587/1729-4061.2015.38963

12. M.V. Zagirnyak, V.V. Prus, and A.V. Nikitina. "Grounds for Efficiency and Prospect of the use of Instantaneous Power Components in Electric Systems Diagnostics." Przeglad Elektrotechniczny 82 (12): 123-125 (2006.)

13. Savchenko, I., Shapoval, A., Kuziev, I. Modeling of high module power sources systems safety processes. (2022) Materials Science Forum, 1052 MSF, pp. 399-404.

14. Savchenko, I., Shapoval, O., Kozechko, V., Markov, O., Hrudkina, N., Voskoboynik, V. Optimization of Informative Signals Stability Along the Waveguides. (2021) Proceedings of the 20th IEEE International Conference on Modern Electrical and Energy Systems, MEES 2021.

15. Hrudkina, N. S., O. E. Markov, A. A. Shapoval, V. A. Titov, I. S. Aliiev, P. Abhari, and K. V. Malii. (2022). "Mathematical and Computer Simulation for the Appearance of Dimple Defect by Cold Combined Extrusion." FME Transactions 50 (1): 90-98. doi:10.5937/fme2201090H

16. O.E. Markov "Forging of Large Pieces by Tapered Faces." Steel in Translation 42 (12): 808-810. (2012.) doi:10.3103/S0967091212120054